EXHIBIT 5

REDACTED VERSION OF DOCUMENT TO BE SEALED

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF MICHIGAN

In re Flagstar December 2021 Data Security Incident Litigation	:	Case No. 4:22-cv-11385

HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY

Videotaped Deposition of

WILLIAM HARDIN

Thursday, November 16, 2023

9:50 AM to 5:33 PM CST

Zoom Remotely Reported by: Melody Stephenson, BBA, FCRR, CRR, CRC, RPR, RSA, MO CCR 406, IA CSR 974

talk to Dillon, but most likely not. I think on your Exhibit 3, the engagement letter's in October. So from that perspective, it looks like the work started in late October.

Q So if you wanted to go back to your firm and figure out what invoices were submitted to Flagstar, that would be something you would consult with Dillon McBride; is that right?

A That's correct. Yes.

Q As you sit here today, you don't have any reason to believe that you or your firm performed work on this matter before October 28th, 2022; is that right?

A That's correct.

Q Okay. I'm handing you what I've marked as Exhibit 5. This appears to be an invoice from December 30th, 2022. Please take a second to review it.

A Sure. Okay.

Q Is this a fair-and-accurate copy of the invoice you submitted on December 30th, 2022?

A Yes, it appears to be that way. Yes.

Q Turning to the last page of Exhibit 5, that lists what's called a "labor detail"; is that right?

MS. SIELING: Ob- --

Q (By Ms. Kane) And --

MS. SIELING: Object to form.

A Yes.

Q (By Ms. Kane) And then I guess I want to ask that a different way. Was the declaration that you previously submitted in another case, was that also related to research on the Dark Web?

A Yes. It was related to that, but it was also related to how a ransomware attack occurred and things of that nature.

Q So the scope of that engagement was a little bit broader?

A Very broad; very dense.

Q Besides the declaration that you've submitted in the other case, have you previously submitted any type of expert reports in any other cases?

A Oh, I don't think so.

Q If you had, would that be something you'd be able to find through searching your files?

A Yes, it would. I -- I don't -- I don't recall anything going into an ex- -- expert report.

Q Does your declaration, Exhibit 2, contain

all of the opinions that you are offering at this stage?

A Yes.

Q To your knowledge, have you developed any opinions in this case that you did not include in your declaration?

A No.

Q So that's a, no, you have not developed any opinions that are not included; right?

A The only opinions I'm including are stated in that report.

Q I understand that you reviewed this report in preparation for your deposition today. Have any of your opinions changed since issuing your declaration?

A No.

Q Is there anything in your declaration that you believe is inaccurate?

A No.

Q Is there any analysis missing from your declaration?

A Not to my knowledge; no.

Q Are there any facts or evidence missing from your declaration?

MS. SIELING: Object to form.

A No.

Q (By Ms. Kane) Is your declaration incomplete in any respect?

A In my opinion, no.

Q If you are called to testify at a hearing or trial in this matter, all of the opinions that you would offer in this case are contained in your declaration; correct?

A Yes.

THE WITNESS: Could I get some more water?

MS. KANE: Let's go ahead and take a break.

VIDEOGRAPHER: Going off the record. 10:43 AM.

(Off the record.)

VIDEOGRAPHER: Going on the record. The time is 10:58 AM.

Q (By Ms. Kane) Mr. Hardin, what was the scope of your assignment in this case?

A The scope of our assignment in this case was to research individuals on the Dark Web to see if their information had been exposed.

Q Were you asked to do anything else?

A We were also asked to see if Flagstar was out there as well.

Q And when you say out there, what do you mean?

A I'm sorry. Out on the Dark Web.

Q So you were also asked to research Flagstar to see if Flagstar's data was on the Dark Web?

A Yes.

Q Could you explain what the Dark Web is?

A Sure. So the Dark Web, to access it, you have to go out and acquire a special browser. That browser is a Tor browser. Tor stands for The Onion Router. It's a non-for-profit organization that's out there. Once you download the browser, then from that perspective, you have to understand where to go and what to do. The Dark Web does not have, like, a search engine per se. There's lots of different sites. As long as you have what's called "the onion link," that takes you out to a site that you can go out to.

In our research, what we end up doing is we go out and look at crime syndicates that we know that are out there and others that allegedly post data of victims. We also go out to different marketplaces that are out there and see if information is out for sale associated with

two major components to it. One was researching certain individuals to see if their information was on the Dark Web; right?

A Mm-hmm.

Q Is that right?

A Yes.

Q And -- and the second component was to see if Flagstar's data was on the Dark Web; is that right?

A That is correct.

Q Were there any -- anything else that you -- let me rephrase. Was there anything else that you were asked to do in the scope of this assignment?

A No.

Q You mentioned that there are different marketplaces on the Dark Web?

A Mm-hmm.

Q Could you sort of give me a bird's eye view of how big the Dark Web is, what the scope of it is? Are there, you know, ten -- ten marketplaces? Are there an unlimited number? Contacts you can provide would be helpful.

MS. SIELING: Object to form.

A Un- -- unlimited. Un- -- unknown.

Q (By Ms. Kane) So there are an unknown unlimited number of marketplaces on the Dark Web?

A Yes. Marketplaces can come and go. It depends on the server that's up there. For example, Monopoly Market, a marketplace that's out there that the FBI and Integral just recently took down. That marketplace was out there for about a year before law enforcement was able to take it down.

Q And when we're talking about marketplaces, do you mean, like, a specific website?

A A specific onion link, yes.

Q And I -- I noticed in your report you reference what's called the "Surface Web"; right?

A Mm-hmm.

Q You also reference the Deep Web and the Deep Dark Web. Could you explain the difference between those three -- what those three things are?

A Sure. I think I outlined that in the report here.

Q And I guess let me rephrase the question, Mr. Hardin. Are -- the Surface Web, Deep Web, and Deep Dark Web, are those all a component of the -- the Dark Web that we're talking about?

of them might be down. Again, it's just going to depend if law enforcement has taken them down or if the site administrator has decided to move the respective link, and then that marketplace shows up in another area.

Q When you're referring to Exhibits B and C, you're referring to Exhibits B and C of your declaration that you've submitted in this case; is that right?

A Yes.

Q So I want to take a look at both of those. The first you mentioned, Exhibit C --

A Yes.

Q -- I'm going to turn to that. And that's Exhibit 2 in this case, but then it's Exhibit C to that exhibit. So you mentioned that this is a list of different crime groups; is that right?

A That -- that's correct; yes.

Q And I see you -- you label them as "ecrime forums" in the exhibit; is that right?

A Yes.

Q So from -- it looks like there are about [redacted] of these crime groups; right?

A At -- at this time, yes.

Q And are those -- there's -- there appears

themselves. So, for example, Number 3, [redacted] [redacted] was the number one crime -- excuse me -- the number one ecrime group for 2022.

Q Mm-hmm.

A They will be the same for 2023. The victims that have chosen not to pay are listed up on their site. So it will have the victim name and potential information associated that they have taken from them.

Q Gotcha.

A And that's the way it works for each one of these. And that's how they brand themselves.

Q So each of these forums that you've listed in Exhibit C, these are cites that the criminals have created to post data or information for folks who have not paid ransom; is that right?

A That is correct. Yes.

Q And then you mentioned that this list reflects the ecrime forums that existed I think at the time you submitted your declaration; is that right?

A That is correct.

Q Do you recall when you prepared this list?

A Most likely in July.

Q Okay. And --

A I think that's when -- if I go back to the invoice that we have here on -- sorry -- Exhibit 7? Did you call it seven?

Q Yes.

A Okay. All right. So on Exhibit 7, that looks like when we were drafting all of this. So yes.

Q So these [redacted] shame sites listed on Exhibit C, those -- those may be different today; right?

A That is correct; yes.

Q And they could've been different at the time that the data incident occurred; is that right?

MS. SIELING: Object to form.

A Yes. Like, today, there's a -- a new ecrime group that's shown up that's called [redacted] will not be on this list because that crime group just formed about ten days ago.

Q (By Ms. Kane) Since you've submitted your declaration, you have not gone back and updated this list; is that right?

A That is correct.

Q Since you submitted your declaration, you

have not gone back and looked at these various shame sites to identify whether Flagstar's data was located on them; right?

A No, I have not.

Q And since you've submitted your declaration, you haven't gone back through the shame sites, the [redacted] shame sites, to identify whether or not any certain individual's information was posted on them; is that right?

A That is not correct. I go out to these shame sites, depending on who my client is, to look for individual information associated with them.

Q Okay. Well --

A If you're asking me specifically have I gone back and looked at these shame sites with this declaration, the answer is no, I have not.

Q Let me ask you this. Since you submitted your declaration in July of --

A Mm-hmm.

Q -- 2023 --

A Yes.

Q -- have you gone back onto each of these shame sites to determine whether or not John Scott Smith's information was found on them?

A Oh, no, I have not.

Q And since you submitted your declaration in July of 2023, have you gone back onto any of these shame sites to determine whether or not Flagstar's data is on them?

A No, I have not.

Q Since you submitted your declaration in July of 2023, have you gone back to search to see whether or not each of these shame sites still exists?

A Yes.

Q And what did you find?

A Some of them are no longer there. Other ones have proliferated. So we have new ones that have come, and we've had others that the onion link no longer works.

Q Do you have an updated list of the shame sites that are currently active?

A Do I have an updated list of shame sites that are currently active?

Q Yes.

A Yes, I do.

Q Zooming out a little bit, is this list of shame sites that's in Exhibit C to your declaration, is this a list that reflects all of

the shame sites that you and CRA had access to as of the time you submitted your declaration?

A Yes. On the ecrime forums, yes.

Q How did you and CRA identify this list of shame sites for use in your declaration?

A Multiple different ways.

Q Could you explain?

[redacted]

Q Mm-hmm.

[redacted]

Q Mm-hmm.

[redacted]

Q Okay.

[redacted]

[redacted]

Q Do you know as of the time that you submitted your declaration in July of 2023 how many shame sites existed on the Dark Web?

A At the time from our research and understanding, there were roughly about [redacted], and that's the number that we have here.

Q Are you offering the opinion today that these [redacted] shame sites are the only shame sites that exist on the Dark Web?

MS. SIELING: Object to form.

A Can you rephrase that question?

Q (By Ms. Kane) Sure. Is it your understanding that the [redacted] shame sites you have list -- you have listed in Exhibit 3 -- or excuse me. Let me rephrase.

Is it your understanding that the [redacted] shame sites listed in Exhibit C to your declaration are the only shame sites that existed on the Dark Web as of July of 2023?

A Those are the ones that CRA monitors. I don't know if there's any other ones out there.

Q So you don't know whether or not there are

additional shame sites that exist on the Dark Web as of July 2023 other than the [redacted] that you've listed here; right?

MS. SIELING: Object to form.

A You're asking me that as of today or as of that particular moment?

Q (By Ms. Kane) Let me rephrase. As of July of 2023 when you submitted your declaration, you only submitted in Exhibit C the shame sites that CRA was aware of; right?

A That is correct. Yes.

Q There may be shame sites that CRA is not aware of; right?

MS. SIELING: Object to form.

A Very low likelihood. But could it be a possibility? Sure.

Q (By Ms. Kane) So as of July of 2023 when you've submitted your declaration, it's possible that there were existing shame sites that you and your staff were not aware of; right?

MS. SIELING: Object to form.

A From a major crime syndicate perspective, we've captured -- we've monitored and captured, I would say, the vast majority of shame sites that are out there.

Q (By Ms. Kane) You say the vast majority, but you can't guarantee that you've captured all of the shame sites that existed as of July 2023 in Exhibit C to your declaration, can you?

MS. SIELING: Object to form.

A No, I cannot.

Q (By Ms. Kane) And that's, again, because the Dark Web is so large in scope; correct?

MS. SIELING: Object to form.

A That -- that is correct.

Q (By Ms. Kane) And you rely on research and work that you do to identify these shame sites; right?

A Yes.

Q You mentioned that these shame sites can be removed from the Dark Web --

A Mm-hmm.

Q -- and change links; right?

A Yes.

Q So do you know if the -- if any of these shame sites that are listed in Exhibit C to your declaration exists but are at different links now?

A Most likely, yes. I'd have to go back through this entire onion link, see if they resolute or not. And if they have an updated

back on.

MS. KANE: Let's go off the record for a moment.

VIDEOGRAPHER: Off the record at 11:17 AM.

(Off the record.)

VIDEOGRAPHER: Going on the record 11:18 AM.

Q (By Ms. Kane) Mr. Hardin, with respect to the shame sites you have listed in Exhibit C to your declaration, I understand you've stated that criminals will use these sites to post the data of individuals or companies that do not pay ransom; right?

A That is correct. Yes.

Q And the purpose is to shame those individuals for not paying ransom; right?

MS. SIELING: Object to form.

A Yes.

Q (By Ms. Kane) Are these forums, in your experience, used for any other purpose?

A No. It's -- it's mostly in the aspect to demonstrate if you choose not to pay or kind of what we call "play their game," then they will victimize you in this way, in other ways that they have as well.

Q So these forums that are listed in Exhibit C to your declaration, they're only used to shame individuals who have not paid a ransom?

A Yes. That and post the information associated with the victim organization.

Q If an organization had paid a ransom, then, you would not expect that organization's data to show up on a shame site; right?

A That is correct.

Q And you mentioned Exhibit B to your declaration?

A Yes.

Q You stated that Exhibit B reflects marketplaces; is that correct?

A That -- that's correct.

Q So these marketplaces are different than shame sites that are in Exhibit C; is that right?

A That is correct. Yes.

Q How are they different?

A So in Exhibit C, that information that's out there is related to that particular ecrime group. Typically, they don't sell data out there. They post the data, and then individuals can download it.

Now, there are some ecrime groups that are

don't sell that data there. Out here, like, for example, if I went out to the [redacted] market, on Number 27, I could find a seller out there that could have VPN credentials. And then once I buy those credentials and validate them, then I could launch an attack. So we have seen in our research and, basically, ecrime forums will use marketplaces to buy certain information in order to attack victims.

Q So these marketplaces that are in Exhibit B, these are some of the websites that threat actors or criminals would use to buy and sell information --

A Yes.

Q -- that's exposed from data breaches, for example; right?

MS. SIELING: Object -- object to form.

A Yes. Yes, they can.

Q (By Ms. Kane) And you mentioned that there are an unlimited number of marketplaces on the Dark Web?

A Mm-hmm. Yep.

Q Here you only have listed [redacted], is that right, or [redacted]?

A Sorry. Hold on. [redacted] Yes.

Q How did you identify these [redacted]?

A Through our research that we do and understanding the proliferation of criminal networks and how they buy and sell goods. What are the most popular forums that out there --

Q Mm-hmm.

A -- and where is the kind of what we call the trust economy at?

Q Mm-hmm.

A Again, remember, criminals rip off criminals on a daily basis.

Q Mm-hmm.

A So these types of forums that are set up are in the aspect of, now, I have someone that has goods for sale. Where -- which marketplace do I trust in order to make a sell?

Q Mm-hmm.

A It's all financial aspects.

Q These [redacted] forums that you have listed on Exhibit B, those are only a fraction of the forums that exist on the Dark Web --

MS. SIELING: Object to form.

Q (By Ms. Kane) -- is that right?

A That's correct. Yes.

Q The links for these forums on Exhibit B,

are they variable? Do they change? Can they be removed? Replaced?

MS. SIELING: Object to form.

A Yes, they can. Marketplaces come and go. Earlier, I talked about Monopoly Market and the FBI taking them down. So once different forums see law enforcement rating, they have to make sure that their site is kind of what we call "bulletproof."

Q Mm-hmm.

A And then the other thing is if they have any inclination that they think they're going to get taken down, they'll move that marketplace to another server so then in turn that the marketplace can be up and going.

Q This list of forums on Exhibit B to your declaration, this is a list of forums that CRA had access to as of the time you submitted your declaration in July of 2023; is that right?

A That is correct. Yes.

Q Since you submitted your declaration in July of 2023, have you updated this list?

A Yes.

Q Does CRA have access to more forums and marketplaces than it -- now than it did in July of

2023?

A Most likely, yes, but I'd have to go back and reconcile to see what our updated lists are.

Q Is it your understanding that any of these marketplaces have been take- -- that are listed in Exhibit B have been taken down or removed since July of 2023?

A I would have to go and reconcile the list to see what's happened.

Q Since you've submitted your declaration in July of 2023, you have not gone back through each of these forums in Exhibit B to see if John Scott Smith's information was on any of these forums; have you?

A No.

Q And since you submitted your declaration in July of 2023, you have not gone back through the list -- in Exhibit B, you haven't gone back through those forums to identify whether or not Flagstar's data is in any of those forums; right?

A That is correct. Yes.

Q You have not gone through any new or additional forums to see if Flagstar's data is listed on those forums since you've submitted your declaration in July of 2023?

A That is correct. Yes.

Q Can you explain -- well, let me ask you this. As part of your work for CRA, do you keep these lists that are in Exhibit B and Exhibit C as a matter of course that you consult in your work for various matters?

A Yes.

Q Who is responsible for updating these lists?

A Multiple people.

Q Is Matt Ahrens one of them?

A Yes.

Q Is Jesse Burke?

A Yes.

Q Are you responsible for updating them as well?

A Yes.

Q How often would you say these lists in Exhibits B and C are updated?

A Probably once we get new information. For example, [redacted] just came online, so that's a new crime group that's out there. So I've updated our list of ecrime forums. So new groups comes up. If a group comes down, we market there. If it changes an onion link, we update it

called a listing of information that they have taken.

And if you remember, back in school, the old Venn diagram, we take circle A, which is our forensics, circle B, which is like threat actor information, and mirror those two together and, hopefully, that they will align. So when I talk about quantify the risk of exposure, that's what we're talking about there.

Q You were not asked to perform that type of work in this case; is that right?

A No, I was not.

Q In performing your work for this case, were you asked to make any assumptions about the facts or the evidence?

A No.

Q Can you explain what opinions you are offering in this case?

A [redacted]

Q Please explain that opinion.

[redacted]

[redacted] So that's an opinion that we're forming.

Q Are you offering any other opinions in this matter?

A Our other opinion, I guess that we're offering, is that the information associated with Flagstar was not posted out on any known shame sites associated with this particular event.

Q Are you offering any other opinions in this matter?

A I -- I don't believe so.

[redacted]

Q [redacted]?

A Yes.

[redacted]

A Mm-hmm.

Q Were you asked to render an opinion about the correlation between those two cyber groups?

A No. We -- we provided that based off our research that we've performed.

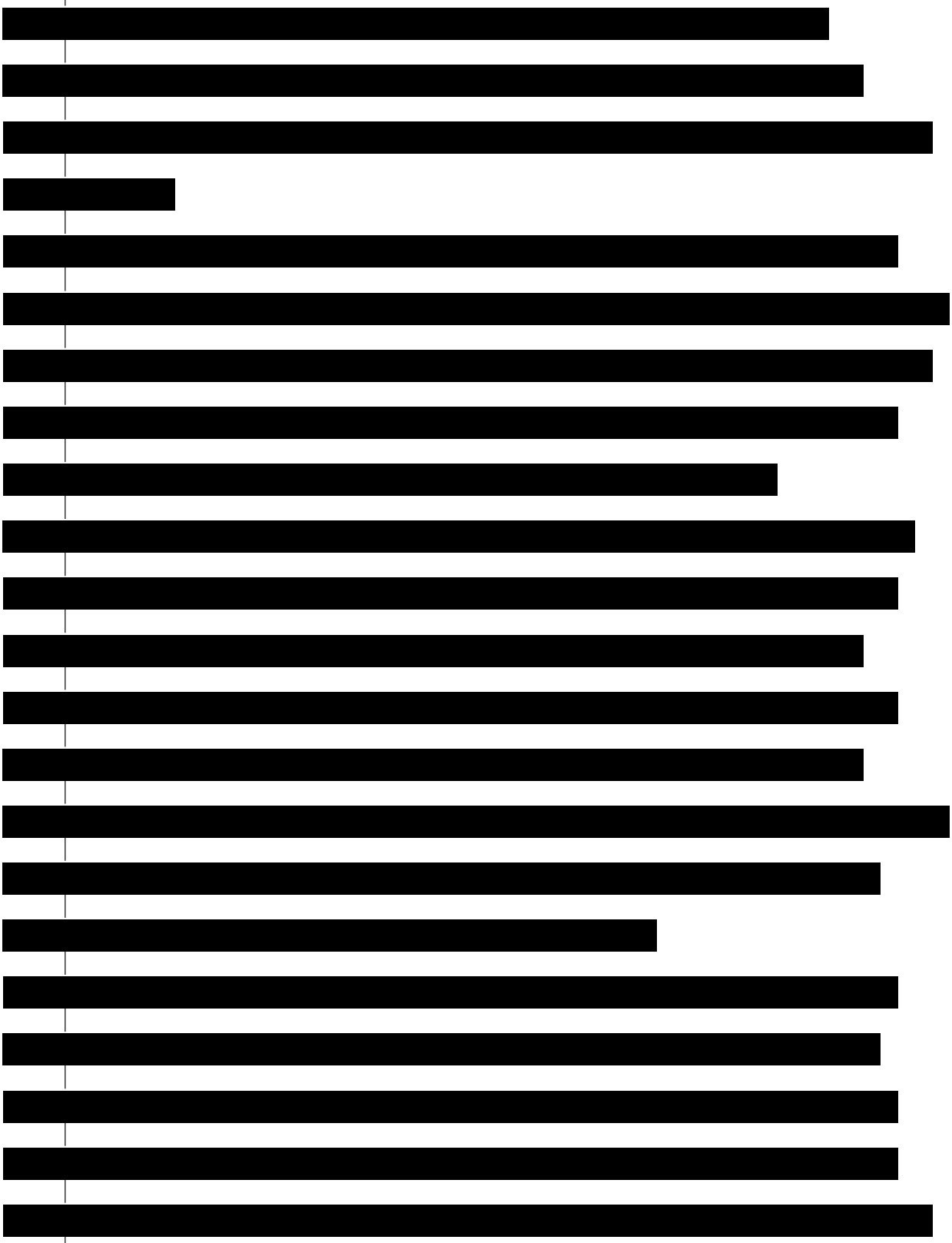
Q Why did you provide that opinion?

A Because it provides context more than anything. The way crime forums work, sometimes you have affiliates or other crime groups that moderate certain forums. So if you can understand the psyche of -- of your adversary, that allows you to understand are they following kind of what we call the pirates code that's out there?

Q What do you mean by "the pirates code"?

A So the pirates code is when you make a ransom payment, will the obligations be fulfilled? For example, will they provide a decryption key? Will they destroy the information that is in their possession? Will they give you a security report? Will they not list you on their shame site? Will they not attack you again? So depending on what

you provide to them, hence, your terms and conditions, will the adversary, or the crime group, follow through in those conditions?



[redacted] When did you perform those engagements if you can recall?

A I'd have to go back and see all the different dates.

Q Do you think it was -- each of those engagements was within the last five years?

A Oh, yes. Yes.

Q Within the last year?

A This is 2023 right now; right? Within the last year? I'd have to go back and take a look, potentially.

Q Within the past two years probably?

A Yes. Yes. Definitely within the last two.

Q So each of the engagements that you've

information on shame sites; is that right?

A That is correct.

Q Okay. Can you explain to me for each of those matters on what the general circumstances were of the negotiations with the threat actor and the ransom payment?

MS. SIELING: Object to form.

Q (By Ms. Kane) Let me rephrase.

A Okay.

Q So you're stating that you recall handling a number of matters, including Shao, and you're relying on your previous experience with Shao as a basis for your opinion in this case; is that right?

A I think what I'm doing is related to that but also all ransom cases that I have performed.

Q Sure. But specific to Shao, are -- you mentioned that the identity of the threat actor is relevant because it, you know, helps provide color to whether or not the threat actor will follow the pirates code; is that right?

A That -- that -- yes.

Q And in your experience with Shao specifically, you believe that the matters that you've worked on have indicated that Shao follows

the pirates code; is that right?

A Yes. I would say that's correct.

Q Okay. But can you give me any specifics of what those matters were?

A I'd have to go back and look at the cases and then refresh myself on them.

Q So as you sit here today, you cannot provide us the details of your experience with Shao; is that right?

MS. SIELING: Object to form.

A I would say with Shao specifically, I'd have to go back and look at my client files to see exactly what happened.

Q (By Ms. Kane) You've handled cases involving ransomware in which Shao has not been the threat actor; right?

A That is correct. Yes.

Q So in your experience negotiating ransomware cases, are there threat actors or threat actor groups that don't follow the pirates code?

A Not that I'm aware of.

Q So in the ransomware cases that you've negotiated, would you say that every ransomware group that -- well, let me rephrase. You've

[redacted]

Q Okay. So --

A And we did not find anything associated with Flagstar.

[redacted]

Q Do you have a list of these search terms that you used or your staff used to search these

marketplaces?

A I'd have to go back and look.

Q Is that something -- is -- a list of the various search terms you used across these marketplaces, is that something that you would've kept in the normal course of your business?

A It depends.

Q Okay. Do you have any idea if you kept that type of list in this case?

A I don't recall.

Q Did you direct your employees, Mr. Burke or Mr. -- your partner, Mr. Ahrens, did you direct them to keep a list of the searches that they performed on these marketplace search engines?

A Keep a list of the searches. Do you mean the -- what they found?

Q The search terms used.

A Oh, the terms? I don't recall.

Q Did you provide any direction to Mr. Burke or Mr. Ahrens regarding what search terms they should use across these search engines on the marketplace?

A No. Both of them are skilled operators. So when we have a task associated with us, you know, it's up to them to determine exactly how

they want to hunt and find information.

[redacted]

Q How would you use the result of a search term?

A It's pretty expansive; isn't it?

Q Right. How --

A Yeah.

Q Yeah. Can you explain to me how you would've used that search term to identify whether or not any Flagstar data was on a marketplace?

[redacted]

Q Can you tell us which marketplaces have that -- have the ability to engage in that way or -- and what marketplaces are just forums that are set up?

A Do you want me to go through the whole list? It's a long process.

Q Well, let's turn to Exhibit B for a second of your declaration.

A Sure.

Q So if I'm understanding correctly, you're sort of making a distinction between two different types of marketplaces. One is a place where

either passing information along or they're trying to capitalize on the information and try to sell the data.

Q So some marketplaces are more like Amazon where it's people interested in selling or purchasing the data go on to the forum and purchase it, sell it, without much engagement; is that right?

MS. SIELING: Object to form.

A That -- that -- that's correct. Yes.

Q (By Ms. Kane) And then some of these Exhibit B marketplaces are more like eBay where you can negotiate or discuss pricing --

A Yes.

Q -- or various assets of the deal with the threat actor; is that right?

A That's correct.

Q Okay. For the -- for the marketplaces that are more like Amazon --

A Mm-hmm.

Q -- for those marketplaces, when you were searching for Flagstar's data, would you just search -- use the search engine that was available on that marketplace to identify whether or not Flagstar's data was available?

A If -- if available, yes. If not, then it's going through forums and things of that nature that are out there to determine, like, who's trying to move what where, what's the history of that person that's there.

Q Did CRA keep any sort of record of how you and your staff conducted this analysis of the Exhibit B marketplaces?

A When you say record, help me out. What is that?

Q Is there any document or material that we could consult to see how you analyzed these various marketplaces to identify whether or not Flagstar's data was actually present on those marketplaces?

A No, there's no written documentation or things of that nature.

Q Turning back to your declaration, if you would, turn to Page 6.

A Sure.

Q Wait. Turn to Page 7.

A Okay.

Q So Paragraph 24 --

A Mm-hmm.

Q -- states that CRA searched for Flagstar

Q Because Flagstar paid a ransom, you would not expect for Flagstar's data to be posted on a shame site; right?

MS. SIELING: Object to form.

A That is correct. Yes. According to the pirates code and reading the communications associated with -- that I was provided and in addition doing all of your searching, we did not see that information out there, but we did find it associated with own Clop. And it's my understanding that Flagstar was part of the Accellion breach that occurred along with numerous other victims that Clop posted up.

Q Your analysis in this case regarding whether Flagstar's data was located on the Dark Web --

A Mm-hmm.

Q -- was limited to October 28th, 2022, to November 14th, 2022; is that right?

MS. SIELING: Object to form.

A That's correct. That's -- that's where we searched for the information during that time window.

Q (By Ms. Kane) CRA only searched for whether or not Flagstar's data was available on

these [redacted] marketplaces between October 28th, 2022, and November 14th, 2022; right?

MS. SIELING: Object to form.

A That is correct. Yes.

Q (By Ms. Kane) So if data related to the data breach was posted and then removed prior to October 28th, 2022, you would not have found it; is that right?

MS. SIELING: Object to form.

A If it was posted and -- clarify your question, please.

Q (By Ms. Kane) Sure. If a threat actor had posted data related to the data breach prior to October 20th, '22, and removed it before October 28th, 2022, you would not have found that data in your search?

MS. SIELING: Objection. Hypothetical. Calls for speculation.

Q (By Ms. Kane) You can answer.

THE WITNESS: Do I answer?

MS. SIELING: You can answer --

THE WITNESS: Oh.

MS. SIELING: -- if you can.

A Okay. Sorry. Can you ask it again?

Q (By Ms. Kane) If a threat actor had

speculation. Asked and answered.

A Again, I -- I just have to clarify it. The way that you're asking the question is if the data had been posted. My answer is the data would not have been posted because a ransom had been paid.

Hypothetically, if a ransom had not been paid and the threat actor did post the data and subsequently removed that information, then, yes, I would not have been able to find anything because our searches would've been through October 28th to November 14th.

Q Your searches would only find data that was available on the Dark Web on those [redacted] marketplaces that was available between October 28th, 2022, and November 14th, 2022?

MS. SIELING: Object to form. Misstates --

A That -- that is our search period of where we looked for information, yes.

Q (By Ms. Kane) So if data was posted after November 14th, 2022, to any of those marketplaces, your analysis would not have included that data; right?

MS. SIELING: Object to form. Calls for

speculation.

A That is correct because we have not searched for anything since that date.

Q (By Ms. Kane) And your search across the [redacted] shame sites was limited to October 28th, 20- -- 2022, to November 14th, 2022; is that right?

A That is our search period, yes.

Q So if any data was posted after November 14th, 2022, to those shame sites, your analysis would not have included or considered that information; is that right?

MS. SIELING: Object to form.

A That -- that's correct. Yes.

Q (By Ms. Kane) And if any information had been posted to those shame sites before October 28th, 2022, and then removed, your analysis would not have captured that information; is that right?

MS. SIELING: Object to form. What do you mean by information?

Q (By Ms. Kane) Let me rephrase. If data had been posted on shame sites related to the Flagstar data breach before October 28th, 2022, and then removed before October 28th, 2022, your analysis would not have picked up if that data was

your opinion that generally speaking, the payment of a ransom guarantees that a -- that the stolen data will not be posted on the Dark Web?

MS. SIELING: Object to form.

A In my opinion, based off all the cases I've worked on, when payment has been made, information has not been leaked.

Q (By Ms. Kane) Are you familiar with the joint Cybersecurity & Infrastructure Security Agency?

A No, I am not.

Q You're not familiar with that group?

A No. Would you like to refresh me?

Q I'm going to hand you what I will mark as Exhibit 8. Go ahead take a look at that.

A Okay.

Q I don't need you to review that, and you can take your time, but I'm going to be asking you about one specific piece of that. Just take a look at it generally.

A Sure. Okay.

Q So this is what's called -- on the front page, it says it's a Stop Ransomware Guide; is that right?

A Yes.

Q And it --

A That's what it says on the document.

Q -- it looks like it was published October 2023 --

MS. SIELING: Object to form.

Q (By Ms. Kane) -- is that right?

A Yes.

Q Have you ever seen this document before?

A First time.

Q Okay. If you go to Page 3 of the document --

A Mm-hmm.

Q -- if you go to the bottom of the page, the last paragraph that starts with "These ransomware and data extortion"; do you see that?

A Where again?

Q The bottom of the page of the last paragraph says, "These ransomware and data extortion prevention and response best practices." Do you see that paragraph?

A Yes, I do.

Q Okay.

A Yeah.

Q It goes on to say "These ransomware and data extortion prevention and response best

practices and recommendations are based on operational insights from CISA, MS-ICAC [sic] --

A Mm-hmm.

Q -- the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI), hereafter referred to as the authoring organizations." Did I read that correctly?

A Yes, you did.

Q Okay. So do you have an understanding of what the CISA is?

A Well, there's a bunch of different definitions of what CISA is. But according to your document, it's the joint Cybersecurity & Infrastructure Security Agency.

Q Are you familiar with that agency?

A I don't believe so.

Q Are you familiar with the NSA?

A Yes.

Q Are you familiar with the FBI?

A Yes.

Q Are those organizations that, from your understanding, have knowledge and provide guidance on how to respond to ransomware and data extortion events?

MS. SIELING: Object to form.

A Depending on the victim, yes.

Q (By Ms. Kane) And does this appear -- I mean, this appears to you to be some sort of guide authored by those agencies regarding ransomware and data extortion prevention and response best practices and recommendations; is that right?

MS. SIELING: Object to form.

A That's what the document says. I can't -- I have -- haven't read it, so I can't give you an opinion on it.

Q (By Ms. Kane) Now, I want to turn on this to Page 21.

A Okay.

Q There's a box on that page starting with "The authoring organizations"; right?

A Yes.

Q So if you sort of cross-check that back with the Page 3 we were just on --

A Okay.

Q -- it defines the authoring organizations as the CS- -- CISA, MS-ISAC, NSA, and FBI.

A Mm-hmm.

Q Do you recall that?

A Yes.

Q This box on Page 21 of Exhibit 8 says,

"The authoring organizations do not recommend paying ransom." Did I read that correctly?

A That is correct.

Q It says, "Paying ransom will not ensure your data is decrypted, that your systems or data will no longer be compromised, or that your data will not be leaked." Did I read that correctly?

A Yes, you did.

Q Do you disagree with this guidance?

MS. SIELING: Object to form.

A It's not that I disagree with that guidance. It's that the problem with that guidance is it's a business decision. Law enforcement will come out and say they don't want to do it because you're enabling this ecosystem. The business has to make a decision if they're going to move forward with a payment.

Q (By Ms. Kane) Mr. Hardin, do you agree with the statement made in this ransomware guide that paying ransom will not ensure your data is decrypted?

MS. SIELING: Object to form.

Q (By Ms. Kane) Yes or no?

A Paying ransom will not ensure your data is decrypted. Well, I disagree with that on the

basis of before any ransom is payment, normally, you will test to make sure that the keys will work.

Q So, Mr. Hardin, you disagree with that statement?

A Paying ransom will not ensure your data is decrypted? Yes, I disagree with that statement.

Q Do you agree with the statement that paying ransom will not ensure that your systems or data will no longer be compromised?

MS. SIELING: Object to form.

A I disagree with that statement as well.

Q (By Ms. Kane) And you also disagree with the statement that paying a ransom will not ensure that your data will not be leaked?

A Based off of that statement and my experience, yes, I disagree with it.

Q So you're offering the opinion in today's case that the ransom payment ensured that the data would not be posted on the Dark Web --

MS. SIELING: Objection.

Q (By Ms. Kane) -- is that right?

A In the cases that I have handled and the payments that I -- have been made, the data of my clients has not been leaked out on the Dark Web.

and the negotiator; right?

A Correct.

Q You did not -- you were not a part of the negotiation with the threat actor; right?

A No, I did not handle this negotiation.

Q You don't have any personal knowledge of -- other than the documents that you reviewed, you don't have any personal knowledge of the negotiations with the threat actor in this case; right?

A No, I do not.

Q Okay. The only documents you've seen related to the terms of the agreement are documents that were provided to you by Flagstar's counsel; is that right?

A That is correct.

Q Now, these terms of the agreement that you listed in Paragraph 14, they include, like we've discussed, access provided to Flagstar to delete the data; right?

A Yes.

Q But they also -- these terms also include other things too; right?

A Yes.

Q They include a promise by the threat actor

Q (By Ms. Kane) Okay. Well, let me ask you this. Well, you say "most likely." What do you mean by that?

A Well, it's most likely.

Q I mean, couldn't the threat actor take the data and just sell it on the Dark Web and make money?

MS. SIELING: Object to form. Hypothetical.

A What forum would he sell it on?

Q (By Ms. Kane) You tell -- any forum. You tell me.

MS. SIELING: Object to form.

A So in an -- in an ecosystem perspective, again, brand is everything.

Q (By Ms. Kane) Well, let me ask you this. Is it possible for the threat actor to sell data anonymously?

MS. SIELING: Object to form.

A Can a threat actor sell data anonymously? Of course, they can. They -- they can set up a various different handle, and from that perspective, they can advertise information that they have for sale.

Q (By Ms. Kane) So a threat actor could

take stolen data, sell it under a different alias; right?

MS. SIELING: Object to form. Hypothetical.

A In a theoretical world, yes, that could occur.

Q (By Ms. Kane) They could sell it under a different alias without risking their reputation?

MS. SIELING: Object to form. Hypothetical.

A Depending on the forum that they're in, likely not.

Q (By Ms. Kane) So in a circumstance, okay, that a threat actor is paid a ransom for stolen data but hold on to that data or wants to try to make more money off of that data --

A Okay.

Q -- okay?

A Yeah.

Q They could take that stolen data and sell it in pieces on the Dark Web; right?

MS. SIELING: Object to form.

A Depending on what the data is, they could, but that -- all that takes time. If you've taken two terabytes of information, you have to then

decipher what data you have. It could be structured data, unstructured data, images, PDFs. The list goes on and on. And then the question's going to be if you have a buyer out there, what are they buying?

Q (By Ms. Kane) So let's focus on the type of data that was at issue in this case. Okay. Do you have an understanding of what type of data was stolen from Flagstar in this data -- in this cyber incident?

A I do not.

Q Are social security numbers a valuable commodity on the Dark -- on the Dark Web?

MS. SIELING: Object to form.

A No.

Q (By Ms. Kane) Your opinion is that social security numbers have no value on the Dark Web?

MS. SIELING: Object to form. That's not what he said.

A Social security numbers can sell anywhere between 10 cents to $3 on the Dark Web depending on the forum that you're on. In addition to that, depending on the reams of SSNs that you buy, it can also reduce the price.

Q Okay. And what's your --

time that you've -- well, in 2021, late 2021, early 2022, are you aware what -- of what marketplaces Shao operated on, if any?

A Yes.

Q What marketplaces were those?

[redacted]

Q Do you know if during the time of the data breach Shao was active on marketplaces that are not included in the list that you gave in Exhibit B?

A They potentially could have, hypothetically. Yes.

Q And in your analysis in this case, you only checked the marketplaces that are listed in Exhibit B; is that right?

MS. SIELING: Object to form.

A Those are the marketplaces that we checked.

Q (By Ms. Kane) [redacted]

[redacted]

[redacted]

MS. SIELING: Object to form.

[redacted]

Q You, again, don't know the individual actors that made up that group; right?

A No, I do not.

Q So those actors could've reorganized into different grounds; right?

MS. SIELING: Objection. Hypothetical.

A When you say "different groups," are you talking about going to different crime syndicates?

Q (By Ms. Kane) They could have created a different crime syndicate, gone to other crime syndicates. You just don't know; is that right?

MS. SIELING: Objection. Calls for speculation.

A That is correct. I do not know.

Q (By Ms. Kane) You don't know if that crime -- the Shao ransom group still exists in the same form it did back in December of 2021; right?

MS. SIELING: Object to form.

A No, I do not.

Q (By Ms. Kane) You don't know what data the Shao ransomware group had or had access to when its onion site went down in November of 2022; is that right?

MS. SIELING: Object to form.

A I don't know what data or what things from an operational perspective Shao has. What I -- what I do know is an agreement was consummated

Q Oh, I see. Okay. So these affiliates of Yanluowang, they were not a part of different ransomware groups?

A Well, I think you have to understand how the threat actor ecosystem works. So if you'll give me a moment, I'll explain.

Q But before you do, and I appreciate the -- the -- the request to explain, and we will get to that, but I wanted to clarify a few things before that might help me here.

A Sure.

Q So your opinion -- or I guess I'll ask you this. [redacted]

Q Is it based on anything else?

A No.

[redacted]

Q (By Ms. Kane) Can you explain that?

A Well, when you look at the pirates code that's associated, are they going to follow the pirates code that's out there? Do they have a brand that they're trying to protect?

When you're negotiating with someone and you can't see 'em face to face and through that perspective you're just dealing with a back-and-forth on either email or talks or telegram or an encrypted chat channel, the question is do I have the trust? Are they going to abide by the terms that we are outlying? We're paying a lot of money for them to abide by those terms.

Q So here, the identity of Shao and the identity of Yanluowang were relevant for you to evaluate whether or not you thought that the

group?

A That is correct.

Q You don't have any understanding of where any data that was held by Yanluowang before they went inactive, any data that they held -- let me rephrase. You don't know what the people making up the Yanluowang ransom group did with any of their data or resources after they expanded?

MS. SIELING: Object to the form.

A I do not.

Q (By Ms. Kane) [redacted]

Q It's possible that they were also active on marketplaces that are not listed in Exhibit B to your declaration?

MS. SIELING: Object to form.

A It is possible.

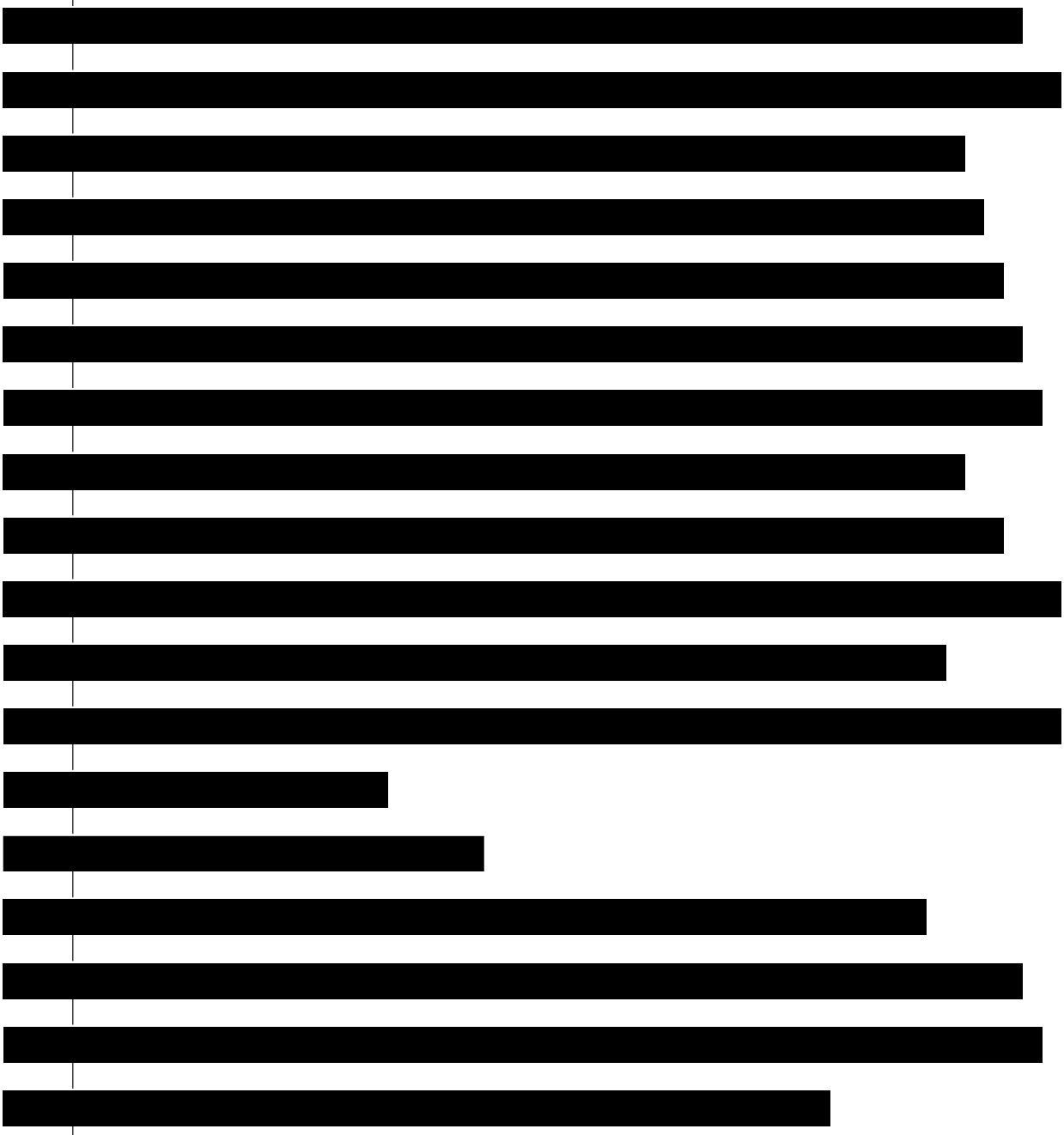
THE WITNESS: What was that?

MS. KANE: I think it's the wind.

MS. SIELING: The wind.

THE WITNESS: Okay.

Q (By Ms. Kane) [redacted]



Q (By Ms. Kane) As you sit here today, you believe that that's an assumption you're making based off of materials and information provided to you by counsel?

MS. SIELING: Object to form.

A I need to go back through my notes, and then I can answer your question.

Q (By Ms. Kane) When you say your notes, what are you referring to?

A Information that I have associated with this particular matter.

Q Are you talking about notes that you created yourself, that you prepared?

A This would be information that I have in my file.

[redacted]

Q (By Ms. Kane) Skipping over to Paragraph 13 of your declaration, the last sentence that starts on Page 4. So "it is unclear if the

[redacted]

Q (By Ms. Kane) Let me ask it in a different way because I think that was a bit confusing.

A Okay.

[redacted]

MS. SIELING: Object to form.

[redacted]

Q (By Ms. Kane) Do you know what that control entailed?

A Control can mean lots of things.

[redacted]

Q In your opinion today, is that -- well, let me -- let's flip to Paragraph 27 of your declaration --

A Sure.

Q -- on Page 8.

A Thank you. Okay.

Q Your declaration, Paragraph 27, states "I opine that Shao kept to the agreement and did not post, sell, or otherwise make available Flagstar's data from the cyber incident"; is that correct?

A That is correct. Yes.

Q You do not opine that Yanluowang abided by any terms of the agreement of Shao and did not post, sell, or otherwise make available Flagstar's data from the cyber incident; is that right?

MS. SIELING: Object to form.

A Well, my adversary in this instance is Shao, based off Exhibit 9, and the agreement and the -- what I opine on is that, yes, they kept to their agreement.

Q (By Ms. Kane) So the answer to my question is, yes, you are not rendering the opinion today that Sh- -- that Yanluowang kept to the agreement or the terms between Shao and Flagstar and did not post, sell, or otherwise make available Flagstar's data --

A There is not agreement --

Q -- excuse me. Let me finish my question, please.

A Sure.

Q -- or otherwise make available Flagstar's data from the cyber incident?

MS. SIELING: Object to form.

A There's no agreement between Yanluo- -- Yanluowang -- sorry. I always -- that's a tongue

twister -- and Flagstar. The agreement is between Shao and Flagstar.

[redacted]

MS. SIELING: Object to form.

[redacted]

Q (By Ms. Kane) You mentioned a couple of times some other threat actor communications that you reviewed between the threat actor and Flagstar in this case; that is right?

A Between the negotiator and the threat actor, yes.

Q Besides the communications with the threat actor and the negotiator and the ransom note in Exhibit 9, did Flagstar's counsel provide you with any other documents to review as background for your analysis?

A No, they did not.

identified suspicious activity on its network which it later identified to be a part of a ransomware attack." Do you see that?

A I do.

Q Do you have any knowledge about the factual basis for that statement?

A No, I do not.

Q You are not offering an opinion today as to when the ransomware attack occurred; right?

A I am not.

Q You're not offering an opinion regarding when data was stolen from Flagstar; right?

A No, I am not.

Q You're not offering an opinion as to what data was stolen from Flagstar?

A I am not, no.

Q Your next sentence states "Flagstar promptly initiated its incident response protocol and took steps to address the incident," right, "including partnering with Kroll to remediate and investigate the situation." Do you see that?

A I do.

Q Okay. You are not offering any opinions in this case regarding the adequacy of Flagstar's data security practices; right?

A I am not.

Q You're not offering an opinion in this case regarding the adequacy of Flagstar's response to the data breach; is that right?

A I am not.

Q I'm going to go down to the second to last bullet point. It says "Flagstar's security vendors continue to monitor the Dark Web, including the site associated with the Shao ransomware group, and have identified no evidence that the threat actors have released any Flagstar data." Do you see that?

A I do.

Q Do you know who the security vendors are that are mentioned in that statement?

A I do not.

Q Did you ask for that information?

A I did not.

Q Why not?

A It's not relevant.

Q It doesn't seem relevant to you whether or not another security vendor or other security vendors identified no evidence that the threat actors released the data?

MS. SIELING: Object to form.

A In this case, yes, I did.

Q Did you review reports from the ransomware negotiators in this case?

A Well, the report to me would be the communications between the threat actor and the negotiator.

Q Did you review reports prepared by any other experts that was retained -- that were retained by Flagstar in this case?

A I did not.

Q Bullet point three on this talking points memo, Exhibit 10, states "Flagstar's systems have since been secured, and all unauthorized access has been revoked since December 2021, which Kroll has independently verified." Do you see that?

A I do.

Q You're not offering an opinion today about when Flagstar's systems were secured?

A I am not.

Q You did not -- you were not asked to verify any of that information?

A I was not.

Q So besides this talking points memo and the threat actor communications, were you provided any other documents by Flagstar's counsel to

email?

A Well, I -- I have --

MS. SIELING: Object to form.

A I have no opinion on that. You asked me to take a look at it. [redacted]

Q If the threat actor had not followed through on the promise to tell Flagstar where the back doors in the networks were -- are or what allowed the threat actor to have access to Flagstar's network, would that impact your analysis?

MS. SIELING: Object to form.

A No, it would not.

Q (By Ms. Kane) And it wouldn't impact your analysis because why?

A Because I was asked specifically to go out to see if Flagstar information was located out on the Dark Web after a payment had been made. That was my objective. The number one objective from my analysis was them demonstrating that that

information had been deleted.

Q Part of your analysis relies on the trustworthiness or credibility of the threat actor that's involved; is that right?

MS. SIELING: Object to form.

A Yes, it is.

Q (By Ms. Kane) And if -- whether or not a threat actor follows through on a specific term and an agreement, that impacts their credibility or trustworthiness; right?

MS. SIELING: Object to form.

A Yes, it does.

Q (By Ms. Kane) So whether or not a threat actor is trustworthy or credible, that's relevant to your analysis; right?

MS. SIELING: Object to form.

A It is relevant, but as I stated in my prior testimony, when you are negotiating with a threat actor, you have to put a risk ranking on the data points that you're going to receive from them. Number one, do I need an decryption key? Number two, data. How am I going to get it back? In our situation here, we looked at the data only, and we made a play for that. They logged in, we made the payment they provided in Exhibit 11.

A Some marketplaces are, yes.

Q And some of the marketplaces on Exhibit B, your declaration, are invite only; right?

A Yes, they are.

Q And so CRA has had to cultivate aliases to acquire access to those marketplaces; right?

MS. SIELING: Object to form.

A Yes, we have.

Q (By Ms. Kane) There are marketplaces that are not on your list in Exhibit B to your declaration that are also invite only; right?

A There can be. Yes.

MS. SIELING: Object to -- object to form.

Q (By Ms. Kane) So there are marketplaces not on Exhibit B that CRA currently doesn't have access to; right?

MS. SIELING: Object to form.

A That is correct, yes.

Q (By Ms. Kane) Do you know how many marketplaces that are invite only that CRA does not have access to?

A I do not.

Q Would it be possible to quantify the number?

A It would not.

Q Why is that?

A Because anybody can do a pop-up marketplace at any time on the Dark Web. It depends. Seller or buyer private forum. The other thing is you've got to realize that law enforcement's always scouring and looking for these marketplaces. They want to take them down. As I stated earlier in my testimony, with Monopoly Market.

Q So marketplaces are constantly changing?

A They are.

MS. SIELING: Object to form.

A Yes.

Q (By Ms. Kane) Including what marketplaces exist that are invite only, right, they constantly change?

A That is correct. Yes.

Q Marketplaces could be put up and taken down on the same day?

MS. SIELING: Object to form.

A Hypothetically, yes.

Q (By Ms. Kane) Put down and taken -- put up and taken down in the same week?

MS. SIELING: Object to form.

A I -- I would say if someone is going to

Q Give me one second. In this email Ms. Sieling lists a number of individuals. Do you see that?

A Yes.

Q Okay. She lists names for -- let's see -- Ms. Saucedo, Mr. Angus, Mr. Smith, and Ms. Robbins; is that right?

A Saucedo, Angus, Smith, Robbins. Yes.

Q Okay. These are the only individuals that you were asked to perform the person of interest analysis for; is that correct?

A That is -- yes. That is correct.

Q And John Scott -- John Scott Smith is the only person from this group who was included in your declaration; is that right?

A That is correct. Yes.

Q You were not asked to complete your person of interest analysis for any of the other named plaintiffs in this case; correct?

MS. SIELING: Object to form.

A No. I was just asked to do the four that are here initially.

THE WITNESS: Sorry. I'm going to drink that water pitcher down.

Q (By Ms. Kane) I'm marking as Exhibit

in your analysis for this case?

A Yes.

Q When did you consult that resource?

A During the time period that I was looking on the Dark Web.

Q Why did you consult that resource?

A That's one of many resources that we take a look at.

Q Did you go to the Shao links site directly?

A No, I did not.

Q Why not?

A Because the site was down.

Q So when you went to search the Shao links site, it actually wasn't accessible, right, directly?

A That is -- that is correct.

Q So you had to instead go through a -- a different resource to try to see what was on Shao links before it became inaccessible; is that right?

A That is correct. Yes.

Q So could you -- I know we discussed this a little bit, but could you describe to me exactly what that resource is that you went to to see what

A No.

Q If you could, turn to Exhibit 13 in front of you.

A Yes.

Q If you could, turn to Page 2 out of 8.

A Sure.

Q The last two entries on that page. The first one's from Tuesday, December 28th at 2020 -- or Tuesday, December 28th, 2021, at 9:10 AM from Flagstar Bank to the threat actor; right?

A Yes.

[redacted]

Q Do you see that? Okay.

A Mm-hmm.

Q There are other things that are said in that as well. The response from the threat actor is on Tuesday, December 28th, at 12:07 PM; right?

A Yes.

[redacted]

Q So the threat actor in this case is under the impression from this communication that they could sell the data anonymously and risk nothing; is that right?

MS. SIELING: Object to form.

A Yeah, I guess.

Q (By Ms. Kane) You don't have any reason to dispute that that's -- that's true?

MS. SIELING: Object to form.

A No. They can go out and do whatever they want with the data.

Q (By Ms. Kane) Mm-hmm. Do You recall in reviewing the threat actor communications that there was a gap in time from when the ransom was paid to when the data that was stolen was accessed by Flagstar?

A I'd have to read through the communication to see if there was such a gap. I -- I can't answer that question.

Q If you could go to --

A One -- one thing I would like to say on that statement that you said "remained completely anonymous and risk nothing," that's more of a proffered statement that threat actors do to get you psychologically thinking they can do things.